# ЧАСТНА ПРОФЕСИОНАЛНА ГИМНАЗИЯ ПО ДИГИТАЛНИ НАУКИ

# „СОФТУНИ СВЕТЛИНА“

# **ДИПЛОМНА РАБОТА**

# ЗА ПРИДOБИВАНЕ НА ПРОФЕСИОНАЛНА КВАЛИФИКАЦИЯ

# НА ТЕМА:

**“Генератор на пароли”**

ИЗГОТВИЛ: НАУЧЕН РЪКОВОДИТЕЛ:

Калоян Коцев Александър Мавродиев

# 

# 03.05.2023 г.

# ГР. СОФИЯ

# **Съдържание**

# 1. Въведение...................................................................................................... 3

2. Типове генератори на пароли...................................................................... 4

3. Описание на функционалността.................................................................. 6

4. Използвани технологии................................................................................ 8

5. Сигурност....................................................................................................... 9

6. Тестове...........................................................................................................10

7.Идея за проекта...............................................................................................11

8. Ограничение и бъдещо развитие..................................................................12

9. Ползи от генератор на пароли......................................................................13

10.Видове кибер атаки и как генераторът се справя с тях.............................15

11. Приложения..................................................................................................20

12. Ръководство за потребителя .......................................................................22

13. Заключение................................................................................................... 23

13. Ресурси.......................................................................................................... 24

**Въведение**

Генераторът на пароли е софтуерен инструмент, който генерира уникални и здрави пароли за потребители. В днешния цифров свят, където всичко - от банкирането до социалните мрежи - се прави онлайн, е от съществено значение да имате силни и сигурни пароли, за да предпазите онлайн акаунтите и личната си информация от неправомерен достъп. Пароли, които са лесни за отгатване или за разбиване, могат да доведат до компрометиране на данните, кражба на самоличност и финансови загуби.

Генераторите на пароли предлагат решение на този проблем, като създават сложни пароли, които са трудни за отгатване или разбиване. Генераторите на пароли могат да създават пароли, които са по-дълги, съдържат комбинация от символи и са напълно случайни, което ги прави по-сигурни от пароли, създадени от самите потребители.

Целта на тази документация е да предостави обзор на инструмент за генериране на пароли, включително неговите функции, функционалност и имплементация. Тази документация е предназначена за всички, които се интересуват от използването или разработването на генератор на пароли, включително спонсори на проекти, разработчици и крайни потребители.

В раздела "Типове генератори на пароли" ще разгледаме различните видове генератори на пароли, включително сложността на генерираните пароли и начините, по които те могат да бъдат използвани. Ще предоставим и сравнителен анализ на различни генератори на пароли, за да ви помогнем да изберете най-подходящия за вашите нужди.

# **Типове генератори на пароли**

Има много различни видове генератори на пароли.

Най-критичният фактор, който трябва да имате предвид, преди да изберете такъв, е къде ще го използвате. Можете да използвате генератор на пароли на всяко устройство, което има достъп до интернет.

Генераторът на псевдослучайни числа (PRNG) - се отнася до алгоритъм, който използва математически формули за създаване на последователности от произволни числа. PRNG генерират поредица от числа, приближаващи свойствата на произволни числа. PRNG започва от произволно начално състояние, използвайки начално състояние. Много числа се генерират за кратко време и могат да бъдат възпроизведени по-късно, ако е известна началната точка в последователността. Следователно числата са детерминистични и ефективни.

Генератор на естествени случайни числа (TRNG)- известен също като хардуерен генератор на случайни числа (HRNG), не използва компютърен алгоритъм. Вместо това той използва външна непредвидима физическа променлива, като радиоактивно разпадане на изотопи или статична вълна, за да генерира произволни числа.

Криптографски защитени генератори на псевдослучайни числа(CSPRNG) - те имат изискванията на CSPRNG попадат в две групи: първо, че преминават тестове за статистическа случайност; и второ, че издържат добре при сериозна атака, дори когато част от тяхното първоначално или работещо състояние стане достъпно за нападател. Случайните последователности, генерирани от всеки CSPRNG, се идентифицират уникално чрез следните три характеристики: (a) висока ентропия; (b) без повторение в генерираните низове; в) нулева корелация.

Grammatical Evolution (GE) е био-вдъхновен инструмент за машинно обучение (ML), базиран на населението, който използва граматиките на Backus-Naur Form (BNF) за генериране на правни структури за различни проблемни области. В тази изследователска работа ние изследваме GE като потенциален източник на ентропия за генериране на първоначално семе с висока ентропия, тъй като всеки еволюционен цикъл е в състояние да произведе различно семе. Ние предлагаме базиран на GE PRNG и базиран на GE CSPRNG, като и двата могат да генерират произволни последователности, които се придържат към покриване на всички стандарти за отлична псевдослучайност.

**Описание на функционалността**

Всички генератори имат едно общо помежду си, те работят, като използват това, което ни е известно като семена.

Генераторите на пароли работят, като използват това, което е известно като семена.

Семената се използват за генериране на случаен низ от знаци, които се използват за създаване на вашата парола.

След като паролата бъде генерирана, семената могат да бъдат изхвърлени, така че да не се налага да я помните.

Начинът, по който се използва семената, ще се различава в зависимост от избрания от вас генератор на пароли.

Някои помощни програми ще използват произволно семе, което не може да бъде предвидено. Други са проектирани с предварително дефинирани алгоритми, които могат да бъдат проектирани обратно, ако някой има достъп до семето, което е използвал за създаване на своите пароли.

Семената се използват за генериране на случаен низ от знаци, които се използват за създаване на вашата парола.

След като паролата бъде генерирана, семената могат да бъдат изхвърлени, така че да не се налага да я помните. Начинът, по който се използва семената, ще се различава в зависимост от избрания от вас генератор на пароли.

Някои помощни програми ще използват произволно семе, което не може да бъде предвидено. Други са проектирани с предварително дефинирани алгоритми, които могат да бъдат проектирани обратно, ако някой има достъп до семето, което е използвал за създаване на своите пароли.

Този проект работи на принципа на генератор на псевдослучайни числа. Функцията (Math.Random), която се използва в проекта за “случайното” генериране на символите, работи с математични формули, за да имитира случайност.

Тези математически формули могат да работят само, ако бъдат зададени периметрите на паролата(букви,цифри,знаци и тн.), за това този тип генератори биват наречени “псевдо генератори”.

Проектът работи като потребителя задава дали ,да има малки и големи букви, да има ли специални знаци, цифри и колко ще е дълга паролата ,за да може тя да работи.

Във следващата част ще бъдат обяснени технологиите ползвани проекта и тяхното предназначение.

**Използвани Технологии**

**1.Javascript**  В този проект Javascript бива използван, за да може генератора да може да изпълнява своите задачи. Интерактивната част на този проект работи като създадем функции, които работят с “аsсii” таблицата, катo чрез функциите “Math.random” и “Math.floor”. Начинът по който генератора създава паролата като първо проверява броя на символите ,после проверява какъв вид символи потребителя задава преди да почне да генерира паролата. Паролата се генерира ,чрез вложен цикъл който оставя само нужните случайни символи.  **2.HTML**  HTML бива използван в този проект, като структура по която да бъдат написани Javascript-a и CSS-a. В него биват създадени: облика на проекта и бутоните които биват натискани ,за да работи.  **3.CSS**

CSS е използван за стила и цвета на проекта. Чрез него също така влиза и библиотеката ”Аnimate” която е използвана за шрифта и снимката на бутона.

**Сигурност**

Не всички „генератори на случайни пароли“ създават наистина произволни резултати. Ако използвам генеричен генератор на произволни пароли, за да създам 10 000 нови пароли, генерираните от мен пароли са резултат от феномен, наречен псевдослучайни, което означава, че резултатите изглеждат произволни, когато всъщност не са.

Стив Уорд, професор по компютърни науки и инженерство в лабораторията по компютърни науки и изкуствен интелект на Масачузетския технологичен институт, казва, че традиционните компютърни системи не са добри при генерирането на произволни резултати. „Те са детерминистични, което означава, че ако зададете един и същи въпрос, ще получите един и същ отговор всеки път“, казва той. „Всъщност такива машини са специално и внимателно програмирани да елиминират произволността в резултатите. Те правят това, като следват правила и разчитат на алгоритми, когато изчисляват.

Според Уорд една напълно детерминистична машина не може да генерира наистина произволни числови последователности, защото следва същия алгоритъм, за да произведе своите резултати. „Обикновено това означава, че започва с общ „начален“ номер и след това следва модел“, казва той. Следователно вашите рандомизирани пароли не са наистина произволни, защото са създадени от същия алгоритъм.

За да може компютърът ми да генерира наистина произволен резултат от хвърляне на зарове, например, компютърът ми трябва действително да хвърли самия зар. Тъй като е изключително трудно да се свърже истински зар с компютър (и очевидният факт, че компютрите нямат ръце), за компютрите е по-лесно да генерират наистина произволни резултати, ако разчитат на непредвидими процеси, като физически феномени: движенията на вашия компютърна мишка, фонов или атмосферен шум, радиоактивен разпад или моментни снимки на лава лампи.

**Тестове**

За тестването този проект бяха изпозлвани методите: debug и unit testing.

**Debug**

Той беше много използван по време на работата по този проект, понеже се стигаше до грешки ,които не можеше да бъдат намерени и се наложи да бъде debug-нато Помогна в изчистване то на много бъгове от проекта.

**Unit testing**

Това беше метода на тестването ,който предимно беше използван по време на писане на дипломната работа. Помогна много, защото в програмата има части от нея ,които са по-лесни за тестване едно ,по едно от колкото да бъде проверявана цялата.

**Идея на проекта**

Проектът е създаден с идеята да даде на хората спокойствие от кибератаките ,които се случват доста често в днешно време . Много хора отделят купища време и пари ,за да са сигурни, че интернет съществуването им да може да мине с възможно най-малко проблеми. Поради тази причина аз реших да създам този генератор на пароли, за да може да се чувствам по спокоен в интернет, без да мисля толкова много за какво може да ми се случи ,ако не съм твърде внимателен.

**Ограничения и бъдещо развитие**

Нищо в програмирането не е ограничено. Един програмист винаги има силата да направи каквото си поиска от нищото. Вярвам, че този проект има много да се развива. Може да се направи да е с криптирани пароли ,може по-хубав интерфейс да му бъде направено и тн.

**Ползи от генератор на пароли**

Създаване на акаунт: Когато се регистрирате за нова онлайн услуга, може да се използва генератор на пароли за създаване на силна и уникална парола за новия акаунт. Това гарантира, че акаунтът започва със стабилна парола, която е устойчива на често срещани атаки, базирани на парола.

Нулиране на парола: Когато нулирате забравена парола, може да се използва генератор на пароли за създаване на нова временна парола. Тази временна парола може да се използва за възстановяване на достъпа до акаунта и потребителят обикновено е подканен да я промени на персонализирана парола при успешно влизане.

Ротация на пароли: Добра практика за сигурност е да променяте паролите периодично. Генераторите на пароли могат да се използват за създаване на нови пароли по време на процеса на ротация на пароли, като се гарантира, че новите пароли са силни и несвързани с предишните.

Системна администрация: Системните администратори често трябва да генерират пароли за различни цели, като създаване на нови потребителски акаунти, предоставяне на временен достъп или конфигуриране на мрежови устройства. Генератор на пароли позволява на администраторите бързо да генерират силни и произволни пароли за тези задачи.

Ключове за криптиране: В системите за криптиране генерирането на парола е от решаващо значение за генериране на силни ключове за криптиране. Ключовете за криптиране се използват за криптиране и декриптиране на чувствителни данни и използването на слаби или предвидими пароли може да компрометира сигурността на процеса на криптиране. Генераторите на пароли могат да генерират сложни и произволни пароли, които служат като силни ключове за криптиране.

Защита на безжична мрежа: Когато настройвате защитена Wi-Fi мрежа, може да се използва генератор на пароли за генериране на силна и уникална парола за протокола за шифроване на мрежата (напр. WPA2, WPA3). Това гарантира, че неоторизирани потребители не могат лесно да получат достъп до мрежата.

Интегриране на приложения: Генерирането на парола е полезно при разработването на софтуер при интегриране с външни услуги или API. Много API изискват използването на API ключове или маркери за достъп, които по същество са пароли. Генераторите на пароли могат да генерират сигурни и уникални ключове или токени за сигурна интеграция.

Одити на сигурността и тестване за проникване: При одити на сигурността и ангажименти за тестване за проникване инструментите за генериране на пароли често се използват за тестване на силата и сигурността на съществуващите пароли в организацията. Генераторите на пароли могат да помогнат при идентифицирането на слаби или лесни за отгатване пароли, които могат да бъдат уязвими за атаки.

**Видове Кибератаки и как генераторът се справя с тях**

**Атаки с груба сила**: При атака с груба сила нападателят систематично опитва всяка възможна комбинация от знаци, докато бъде намерена правилната парола. Този метод отнема време, но може да бъде ефективен срещу слаби пароли или когато атакуващият има значителна изчислителна мощност.

Този генератор не е много полезен срещу този тип атаки, но също така е и достатъчно сигурен ,защото ако някой човек се опита да ни вземе паролата по този начин ще му отнеме твърде много време.

**Атаки с речник**: При атака с речник нападателят използва предварително компилиран списък с общи пароли, известен като речник, и систематично тества всяка парола срещу целевия акаунт. Много хора използват лесни за отгатване пароли, като например „парола“ или „123456“, което ги прави уязвими за този тип атаки.

Този генераторът на пароли може да помогне за защита срещу речникови атаки. Речниковите атаки включват систематично изпробване на списък с често използвани пароли или думи от речник, за да се познае паролата. Ето как генераторът на пароли може да помогне:

**Уникални и произволни пароли**: Генераторът на пароли може да създава пароли, които са уникални и не се основават на общи думи, намерени в речниците. Вместо да използва предвидими думи или фрази, генераторът генерира пароли с комбинация от произволни знаци, числа и специални символи. Това затруднява нападателите да отгатнат паролата, като просто опитват общи думи от речника.

**Повишена сложност**: Генераторите на пароли могат да създават пароли с високо ниво на сложност. Чрез включването на комбинация от главни и малки букви, цифри и специални знаци, генерираните пароли стават по-устойчиви на атаки в речника. Добавената сложност прави по-трудно за нападателите да отгатнат паролата въз основа на често използвани думи или модели.

**Съображения относно дължината**: Генераторите на пароли често позволяват на потребителите да определят желаната дължина на паролата. По-дългите пароли обикновено са по-сигурни, защото увеличават общия брой възможни комбинации, което отнема повече време на атакуващите да извършат успешна речникова атака. Чрез генериране на пароли с достатъчна дължина, генераторът на пароли помага за смекчаване на ефективността на атаките в речника.

Въпреки че генераторът на пароли може да направи значително по-трудно за атакуващите да разбият пароли с помощта на речникови атаки, все пак е важно да използвате други мерки за сигурност, като редовно актуализиране на пароли, активиране на многофакторно удостоверяване и предпазливост при опити за фишинг.

**Фишинг**: Фишинг атаките включват подмамване на потребителите да разкрият своите пароли, като се представят за надеждно лице. Нападателите могат да изпращат измамни имейли или да създават фалшиви страници за вход, които изглеждат идентични с легитимните уебсайтове. Когато потребителите въвеждат своите пароли на тези измамни сайтове, нападателите улавят информацията.

Генераторът на пароли не е много полезен срещу Фишинг атаките защото, за да сработи една Фишинг атака трябва човекът да си даде паролата на друг човек. Поради тази причина сложността на паролите не е от значение. Ако искаме да се предпазим от този вид атаки трябва да внимаваме каквъ сайтове посещаваме.

**Keylogging**: Keyloggers са злонамерени софтуерни или хардуерни устройства, които записват всяко натискане на клавиш, което потребител прави на своя компютър или мобилно устройство. Чрез улавяне на паролата, докато е въведена, нападателите могат да получат идентификационните данни за вход на потребителя без тяхно знание.

Този генераторът на пароли може да помогне за защита срещу атаки за записване на клавиатури. Ето как:

**Избягване на ръчно въвеждане**: Когато използвате генератор на пароли, обикновено не е необходимо да въвеждате ръчно генерираната парола в целевата система. Вместо това можете да го копирате и поставите от генератора на пароли в полето за парола. Това заобикаля способността на keylogger да улавя натискания на клавиши, тъй като паролата не се въвежда на физическата клавиатура.

**Сложност и произволност**: Генераторите на пароли могат да създават силни и сложни пароли, които е трудно за нападателите да отгатнат. С помощта на генератор на пароли можете да генерирате пароли с комбинация от главни и малки букви, цифри и специални знаци. Повишената сложност на паролата прави по-трудно за кийлогърите или нападателите да я разберат или разбият.

**Уникални пароли**: Генераторите на пароли също могат да помогнат за създаването на уникални пароли за всеки акаунт или услуга, които използвате. Това е важно, защото ако един от вашите акаунти бъде компрометиран поради кийлогър или друга атака, уникалните пароли за другите ви акаунти остават защитени.

Въпреки че използването на генератор на пароли може да помогне за намаляване на риска от кийлогъри, които прихващат пароли, важно е да останете бдителни за цялостната сигурност на компютъра и акаунта. Това включва поддържане на устройствата ви защитени с актуален софтуер за сигурност, предпазливост при опити за фишинг и редовно наблюдение на вашите акаунти за всяка подозрителна дейност.

**Пълнене на идентификационни данни**: Тази техника включва използване на откраднати комбинации от потребителско име и парола от един уебсайт за получаване на неоторизиран достъп до други сайтове. Тъй като много хора използват повторно пароли в множество акаунти, нападателите могат да се възползват от тази практика, като използват автоматизирани инструменти за тестване на тези откраднати идентификационни данни на различни платформи.

Това е още един вид атака където генератора на пароли не е толкова полезен колкото да внимаваме колко пъти си повтаряме паролите в различни сайтове. Генераторът тук помага със създаването на нови сигурни пароли.

**Rainbow Table Атаки**: Rainbow Table е предварително изчислена таблица с криптирани пароли и съответните им версии в обикновен текст. Нападателите използват тези таблици, за да намерят бързо оригиналните пароли, съответстващи на съхранените хешове, особено когато се използват слаби алгоритми за хеширане.

Този енераторът на пароли може да помогне за защита срещу атаки на таблицата на дъгата, все още е от решаващо значение да следвате други най-добри практики за сигурност. Те включват използване на силни алгоритми за криптиране за съхранение на пароли, прилагане на подходящи техники за хеширане на пароли (като използване на бавни и скъпи от изчислителна гледна точка алгоритми за хеширане) и редовно актуализиране на пароли за поддържане на силна защита срещу различни техники за кракване на пароли.

**Социално инженерство**: Социалното инженерство включва манипулиране на хора за разкриване на паролите им или заобикаляне на мерките за сигурност. Нападателите могат да се представят за персонал от техническата поддръжка, служители на компанията или доверени лица, за да заблудят потребителите да разкрият паролите си доброволно.

Този Генератор на пароли ,не се справят добре срещу този тип атаки, тъй като дори да имаме добре развита парола , за да сработи социалното инженерство ,означава че потребителят сме дали нашата парола на човека ,който се опитва да я вземе от нас.

**Сърфиране през рамо**: Сърфиране през рамо се отнася до акта на наблюдение на някой, който въвежда паролата или ПИН кода си, като гледа през рамо. Нападателите могат физически или дистанционно да наблюдават хората, които въвеждат паролите си на обществени места или дори да заснемат видеозаписи, за да получат достъп до техните акаунти.

Този генератор на пароли не помага срещу този тип кибер атаки ,защото ,за да сработи този тип атака това означава ,че потребителят е въвел паролата си на публично място без да внимава ,дали има човек, който иска да ни открадне паролата по този начин.

**Приложения**

Генераторите на пароли са ценни по няколко причини.

Те ни позволяват да създаваме дълги, сложни пароли. Генераторите на пароли също са от полза, ако имате проблеми с измислянето на пароли, които отговарят на специфични изисквания (напр. поне 12 знака, цифри, символи и т.н.).

Те ви позволяват да създавате различни пароли за различни уебсайтове, така че ако един бъде компрометиран, останалите да останат в безопасност. Това може да помогне за предотвратяване на хакерите да пробият една система и да получат достъп до всичките ви акаунти.

Най-важното е, че генераторите на пароли са широко достъпни в различни компютърни платформи. Те могат да бъдат достъпни от уебсайтове, настолни компютри, лаптопи, таблети, смартфони и други мобилни устройства.

Това е особено важно, ако често влизате в интернет от обществени компютри. Когато случаят е такъв, често сте принудени да създавате слаби пароли или рискувате системният администратор да излезе от системата.

**Случайност**: Генераторите на пароли могат да генерират пароли, които са наистина произволни. Случайността е от решаващо значение за сигурността на паролите, тъй като предвидимите или лесно отгатваемите пароли са по-уязвими от атаки. Генераторите на пароли използват алгоритми, които създават пароли без забележими модели, което ги прави по-трудни за разбиване.

**Сложност**: Генераторите на пароли могат да създават пароли, които са сложни и трудни за отгатване. Сложните пароли обикновено включват комбинация от главни и малки букви, цифри и специални знаци. Като използвате генератор на пароли, можете да гарантирате, че вашите пароли отговарят на изискванията за сложност, определени от различни услуги и системи.

**Дължина**: Генераторите на пароли ви позволяват да създавате пароли с определена дължина. По-дългите пароли обикновено предлагат по-добра сигурност, тъй като увеличават размера на пространството за пароли, което прави атаките с груба сила по-отнемащи време. С генератор на пароли можете да генерирате пароли с достатъчна дължина, за да подобрите сигурността си.

**Удобство**: Измислянето на силни и уникални пароли за всеки акаунт може да бъде предизвикателство, особено ако имате няколко акаунта. Генераторите на пароли облекчават тежестта на необходимостта сами да измисляте пароли. Те могат бързо да генерират сигурни пароли при поискване, спестявайки ви време и усилия.

**Избягване на лична информация**: Много хора са склонни да използват пароли, които са свързани с личната им информация, като имена, рождени дати или адреси. Тези типове пароли могат лесно да бъдат отгатнати от нападателите, използващи техники за социално инженерство или чрез използване на публично достъпна информация. Генераторите на пароли елиминират използването на лична информация, осигурявайки допълнителен слой сигурност.

**Уникални пароли**: Важно е да използвате уникални пароли за всеки акаунт, за да сведете до минимум въздействието на потенциален пробив в сигурността. Генераторите на пароли могат да помогнат за генерирането на голям брой уникални пароли без повторение. По този начин, дори ако един от вашите акаунти е компрометиран, нападателят няма да има достъп до всички останали ваши акаунти.

**Сигурно съхранение**: Много генератори на пароли също предлагат опцията за сигурно съхраняване на генерираните пароли. Тази функция гарантира, че не е необходимо да помните ръчно всичките си сложни и уникални пароли. Вместо това можете да разчитате на мениджър на пароли или криптирано хранилище, осигурено от генератора на пароли, за да запази паролите ви в безопасност.

**Kaк Работи**

**(Ръководство за потребителя)**

Кодът работи като от Html-a инициализира полетата и бутоните, javascript-а инициализира промените и върши работата на проекта а CSS-a е за дизайна на проекта. Във HTML имаме въведени 6 бутона и едно поле където изписва резултата от получената парола. 4 от бутоните са тикчета и не вършат нищо освен да казват на програмата да не слага тaкива символи в паролата. Другите два бутона са бутоните Generate Password и бутона за копиране.

В javascript-a може да видим интерактивната част от проeкта. Вътре в него има инициализирани DOM променливи, че да може да се достъпва с html-a .Към тях има функции, които помагат за избирането на знак чрез ”ascii” таблицата, която им помага да извадят съответният знак. С константата randomFunc биват инициализирани всички функции. Във конструкцията на кода също така има два EventListener-a , които ни помагат с натискането на бутоните. Единият е за копиране на получената от потребителя парола. В същия EventListener също така излиза и нотификация при копиране на паролата. Другият е за генерирането на паролата. При генерирането на паролата трябва да бъде направена проверка . Проверка през която трябва да се премине, е дали типът данни и дължината, които един потребител може да изисква. След като се мине през тази проверка приложението минава през вложен цикъл който пълни символите в масив. Тези символи след това биват slice-нати от 0 до дължината на паролата. И накрая тя бива изпринтирана.

В CSS-a бива взета библиотеката”animate” за шрифта и за снимката на бутона за копиране. Там също може да видим и цветовете използвани за проекта. Чрез CSS-a проекта получава своя лилав цвят.

За стартиране изберете файла „index.html“. Изберете дължина на паролата и посочете какво да съдържа. След това натиснете бутона „Generate Password”.

**Заключение**

Паролите са жизнено важна част от нашето съществуване в 21 век, ако не държим ние на тях, няма кой друг. Заради това аз реших да направя този генератор на псевдослучайни пароли, че да се чувстваме по-спокойно, докато бърникаме из интернет. Ако един човек отделяше толкова време на паролите си, колкото на телефона си, кибер атаките най-вероятно щяха да са намалели драстично, до сега.

**Препратки**

* Password Generators – What They Are and Why You Need One (<https://www.passcamp.com/blog/the-complete-guide-to-password-generators-what-they-are-and-why-you-need-one/> )
* A random password generator is a software program, hardware device, or online tool that automatically generates a password using parameters that a user sets, including mixed-case letters, numbers, symbols, pronounceability, length, and strength. (<https://www.dashlane.com/blog/how-random-password-generators-work>)
* QUANTUM RANDOM NUMBER GENERATOR - Knowledge Share is an IP platform designed to facilitate the interaction between university technology transfer offices, academic researchers and industry partners, by providing a portal that enables users to easily access information related to patents and technologies that represent the excellence of the scientific know-how in Italy. (<https://www.knowledge-share.eu/en/patent/quantum-random-number-generator/?gclid=Cj0KCQjwr82iBhCuARIsAO0EAZyv-B3zX8HiI23Y-1Fw5W8RcqUPwJy3Zjw14kFHAmIjfvvyZ5Io2iIaAnUpEALw_wcB>)
* Design of a cryptographically secure pseudo random number generator with grammatical evolution (<https://www.nature.com/articles/s41598-022-11613-x>)
* MDN Blog - Resources for Developers, by Developers (<https://developer.mozilla.org/en-US/docs/Web/JavaScript/Reference/Global_Objects/Math/random>)
* Pseudo Random Number Generator(PRNG) (<https://www.geeksforgeeks.org/pseudo-random-number-generator-prng/>)
* RiderFlow for Unity (<https://codemyui.com/>)
* Stack Overflow (<https://stackoverflow.com/>)